Trust Establishment in Cooperating Cyber-Physical Systems

Andre Rein[1], Roland Rieke[1 2], Michael Jäger[3], Nicolai Kuntze[1], Luigi Coppolino[4]

[1] Fraunhofer Institute SIT, Darmstadt, Germany
[2] Philipps-Universität Marburg, Germany
[3] Technische Hochschule Mittelhessen, Giessen, Germany
[4] Universita degli Studi di Napoli "Parthenope", Napoli, Italy

Abstract. Cooperating systems are systems of systems that collaborate for a common purpose. In this work, we consider networked cooperating systems that base important decisions on data gathered from external sensors and use external actuators to enforce safety critical actions. Typical examples of cooperating cyber-physical systems are critical infrastructure process control systems. Such systems must not only be secure, they must be demonstrably so. Using the example of a hydroelectric power plant control system, this paper analyzes security threats for networked cooperating systems, where sensors providing decision critical data are placed in non-protected areas and thus are exposed to various kinds of attacks. We propose a concept for trust establishment in cyber-physical cooperating systems. Using trusted event reporting for critical event sources, the authenticity of the security related events can be verified. Based on measurements obtained with a prototypical realisation, we evaluate and analyze the amount of overhead data transmission between event source and data verification system needed for trust establishment. We propose an efficient synchronisation scheme for system integrity data, reducing network traffic as well as verification effort.

Keywords: trustworthy event management in cyber-physical systems; security of cooperating systems; trusted event reporting; critical infrastructure protection.

1 Introduction

Cooperating Cyber-Physical Systems (CPS) are systems of systems that collaborate for a common purpose. Systems in the physical world are linked to the cyber world by elements such as sensors, which capture data from the physical world and produce information that provides an abstraction of the state of the physical world for processing in the cyber world. Analysis of this information may lead to decisions in the cyber world. These, in turn, influence the physical world either directly, e.g., by actuator elements, or indirectly, e.g., by visualizing information for human actuators in the physical world. Prominent examples for novel cooperating CPS are future smart energy systems, vehicular ad hoc networks, air traffic management systems, and ecosystems for smart cities, which extend the cooperation of networked systems with cross-infrastructure interdependencies.

Obviously, a certain level of trust in these emerging CPS is indispensible and, thus, adequate security concepts are utmost important for common acceptance of these systems.

In smart energy systems, increased interconnection and integration introduces cyber vulnerabilities into the grid that do not yet exist in the current, rather fragmented grid infrastructure [37, 10, 13]. In the case of vehicular ad hoc networks, user safety is a major challenge with great impact on the security of these CPS [11]. Distributed air traffic management systems that collaborate for a common purpose, such as the smooth running of an airport, need continuous update and improvement to security [14]. New challenges with respect to smart city management comprise the provision of trustworthy shared information for cross-application use, the secure data exchange between devices and their users, and the protection of vulnerable devices [3].

As outlined above, sensors are important interfaces, connecting physical and cyber world. Thus, one important requirement common to all application domains of CPS is *the capability to prove that a measured value has been acquired at a certain time and within a specified "valid" operation environment*. Authenticity of such measures can only be assured together with authentication of the used device itself, it's configuration, and the software running at the time of the measurement. A similar requirement is necessary for cyber-controlled actuators in the physical world, namely, *the capability to prove that the actions triggered by decisions taken in the cyber world are executed at the scheduled time and within a specified "valid" operation environment*.

A specific problem in geographically dispersed infrastructures is that the interfaces connecting physical and cyber world are often placed in non-protected environments and attackers are able to access and manipulate this equipment with relative ease [42]. Therefore, when physical access to critical devices cannot be inhibited, *an effective security solution must address detection of manipulations*. Manipulated equipment can be used to cause misjudgement on the physical system's state and hide critical conditions, which in turn can lead to wrong decisions with severe impact on the overall CPS.

In this work, we analyze security threats for critical CPS by means of a representative example, namely, a hydroelectric power plant in a dam. We elicit adequate security requirements based on safety considerations and present a concept for trustworthy event reporting.

Digital signatures obviously can provide authenticity and integrity of recorded data [4]. However, a signature gives no information about the status of the measurement device at the time of measurement. Our solution, the *Trusted Information Agent* (TIA), is based on trusted computing technology [21] and integrates industry approaches to the attestation of event reporter states. We determine the overhead for trust establishment in the amount of transferred data and the calculation cost on the verifier and propose a scheme that efficiently handles the transmission and processing of the stored measurement log produced by the integrity measurement architecture.

The remainder of this paper is organized as follows: Section 2 introduces an exemplary application scenario, discusses security-related challenges for CPS and corresponding security requirements. Based on these requirements, we address a solution for our propositions and describe the concept of a TIA in Section 3. In Section 4, we analyze important scalability aspects of our approach based on a quantitative evaluation and propose a scheme for minimizing the overhead of trusted event reporting. Section 5 gives an overview of the related work and Section 6 concludes the paper and outlines directions for future research.

2 Application Scenario

Our security analysis is based on examples from a hydroelectric power plant in a dam, which is in many respects typical for a critical infrastructure. A dam is a layered CPS with intra- and cross-layer dependencies and with various other sources of complexity. Several distinct functionalities influence controlling and monitoring activities. Moreover, different components, mechanisms, and operative devices are involved, each one with different requirements in terms of produced data and computational loads. A huge number of parameters must be monitored in order to guarantee safety and security.

Among the most commonly used dam instrumentation sensors are water level sensors, thermometers, tiltmeters (measurement of wall or earth inclination), piezometers (water pressure), crackmeters (wall crack enlargement), pressure cells (concrete or embankment pressure), jointmeters (joint shrinkage), and turbidimeters (fluid turbidity). The heterogeneity of currently used devices is a relevant challenge in the dam process control: they range from old industrial control systems, designed and deployed over the last 20 years and requiring extensive manual intervention by human operators, to more recently developed systems, conceived for automatic operations (SCADA).

Indeed, the trend of development is toward increasingly automated dam control systems. While automation leads to more efficient systems and also prevents operating errors; on the downside, it poses a limit to human control in situations where an operator would possibly foresee and manually prevent incidents.

The remote management of such an infrastructure would require a hierarchical SCADA system (cf. Figure 2). The SCADA infrastructure gathers information from individual sensors manged by a Remote Terminal Unit (RTU). At regional level information is managed by a local Master Terminal Unit (MTU) and sent to a central MTU at the remote control center. Each MTU provides a Human Machine Interface useful to manage the controlled system.

Fig. 1: Details of the Monte Cotugno dam: one of the eight dams managed by EIPLI.

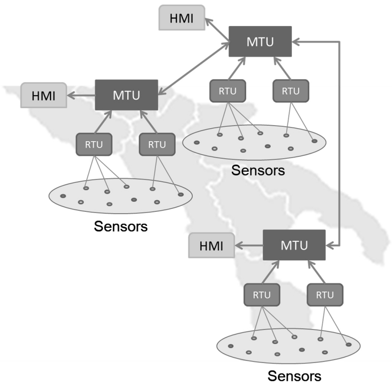


Fig. 2: Deployment of a SCADA system for monitoring a water management infrastructure

Table 1: Security related scenarios and the respective monitoring

Event	Impact	Detection
Changes in the flow levels of the seepage channels	Seepage channels are monitored to evaluate the seepage intensity. A sudden change in flow levels could show that the structure is subject to internal erosion or to piping phenomena. This event can be the cause of dam cracks and failures.	A weir with a known section is inserted into the channel. The water level behind the weir can be converted to a flow rate.
Gates opening	Gates opening must be operated under controlled conditions since it may result in: i) Flooding of the underlying areas; ii) Increased rate of flow in the downstream and catastrophic flooding of down-river areas.	A tiltmeter (angle position sensor) can be applied to the gate to measure its position angle.
Vibration level changes	Increased vibrations of the infrastructure or the turbines can anticipate a failure. Possible reasons include: i) earthquakes); ii) unwanted solicitations to the turbines.	Vibration sensors can be installed over structures or turbines to measure the stress level.
Water levels above alert thresholds	Spillways are used to release water when the reservoir water level reaches alert thresholds. Otherwise, the water overtops the dam resulting in possible damage to the crest.	Water level alarm helps detect unexpected discharge or other anomalous behaviour.

As a severe disadvantage, increased automation and remote control raise a new class of security-induced safety issues, i.e., cyber attacks against the IT layer of the dam could ultimately result in damage to people and environment. Dam monitoring aims towards identifying anomalous behaviour related to the infrastructure. Table 1 summarizes a list of possible scenarios illustrating the necessity of monitoring specific parameters.

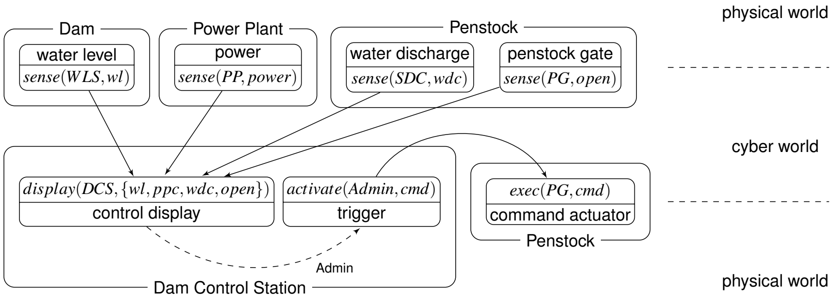


Fig. 3: Interfaces connecting physical and cyber world with functional dependencies

Figure 3 shows some of the functional dependencies between sensors, control station components, and actuators. Dam administrator decisions depend on the displayed measurements, whereas control display values are derived from the sensor measurements. The overall function of the system requires authenticity of measurement values for several critical sensors.

3 Trusted Information Agent

There is no point in monitoring large systems without having a certain level of confidence in the correctness of the monitoring data. To achieve this confidence, network security measures and provisions against technical faults are not enough. In order to address the serious problem of unrevealed manipulation of monitoring equipment, we now describe the concept of a *Trusted Information Agent* (TIA). According to [33], an *agent* is characterized by perceiving its environment through sensors and acting upon the environment through effectors. In this work, we address specific security aspects of these basic functionalities of an agent. The TIA concept is well-suited for a range of device types, in particular, for networked sensor and actuator devices, which are supposed to be critical for a cyber-physical system.

3.1 Trust Architecture

An approved technique to reveal software manipulation is software measurement: Each software component is considered as a byte sequence and thus can be measured by computing a hash value, which is subsequently compared to the component's reference value. The component is authentic, if and only if both values are identical. Obviously, such measurements make no sense if the measuring component or the reference values are manipulated themselves. A common solution is to establish a chain of trust: In a layered architecture, each layer is responsible for computing the checksums of the components in the next upper layer. At the very bottom of this chain a dedicated security hardware chip takes the role of the trust anchor.

Trusted Computing technology standards [21] provide a suitable trust architecture on top of a Trusted Platform Module (TPM). A TPM chip is equipped with several cryptographic capabilities like strong encryption, digital signatures, and some more advanced features. It is also hardened against physical attacks. TPMs have been proven to be much less susceptible to attacks than corresponding software-only solutions.

The key concept is the extension of trust from the TPM to further system components. This is used to ensure that a system is and remains in a predictable and trustworthy state and thus produces authentic results. Even very complex sensors and actuator devices are well-suited for this kind of integrity check concept. The proposed device architecture is presented in more detail now on the example of a trusted sensor device.

3.2 Trusted Sensor Data Aquisition

Figure 4 depicts an architecture for trusted sensor data aquisition consisting of a TIA and several infrastructure systems providing certification, verification and storage services. Those infrastructure components will typically be operated in protected environments, e.g., be all part of the same SCADA control center. The task of a TIA is to gather and report sensor data. Trusted data aquisition means revelation of any software manipulations of the device itself, authenticating the identity of the TIA, and protecting the sensor data against tampering attemps.

The TIA is expected to operate in unprotected environments with low physical protection and externally accessible interfaces such as wireless networks and USB

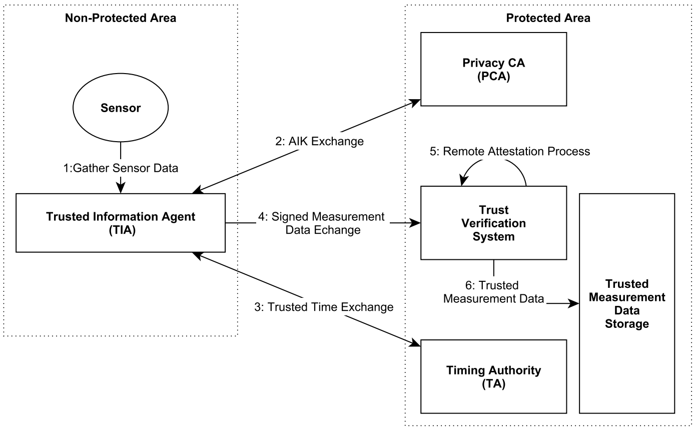

Non-Protected Area
Protected Area
Sensor
1:Gather Sensor Data
Trusted Information Agent (TIA)
2: AIK Exchange
Privacy CA (PCA)
5: Remote Attestation Process
4: Signed Measurement Data Echange
Trust Verification System
3: Trusted Time Exchange
6: Trusted Measurement Data
Trusted Measurement Data Storage
Timing Authority (TA)

Fig. 4: TIA architecture

access for maintenance. A necessary precondition to guarantee authenticity of the measures is a trustworthy state of the measurement device. To meet this requirement, the TIA is equipped with a TPM as trust anchor and implements a chain of trust [18]. Revelation of software manipulations is based on the comparison between the software checksums and the corresponding reference values by a remote verification system (remote attestation) [21].

In addition to the verification system, two infrastructure components are necessary to establish the authenticity of the gathered data. The TIA uses a TPM-generated *attestation identity key* (AIK) as a digital signature key. A *privacy certificate authority* (PCA) issues a credential for this AIK. The certified AIK is, henceforth, used as an identity for the TIA. According to TCG standards, AIKs cannot only be used to attest origin and authenticity of a trust measurement, but also, to authenticate other keys and data generated by the TPM. However, the AIK functionality of a TPM is designed primarily to support remote attestation by signing the checksums of the TIA's software components, while signing arbitrary data is, in fact, not directly available as a TPM operation. We have shown elsewhere, how to circumvent this limitation [17]. Hence, we are able to use TPM-signatures for arbitrary data from the TIA's sensors.

Furthermore, a *time authority* (TA) is needed to approve the correctness of the measurement time stamps. Any TPM is equipped with an accurate timer. Each event signature includes the current timer value. However, the TPM timer is a relative counter, not associated to an absolute time. The TA issues a certificate about the correspondence between a TPM timestamp (tickstamp) and the absolute time. The combination of tickstamp and TA-certificate can be used as a trusted timestamp. Alternatively, another trusted time source, such as GPS, could have been used.

Putting it all together, a measurement record includes arbitrary sensor data, a TA-certified time stamp, and a hash value of the TIA's software components. The record itself is signed by the PCA-certified AIK.

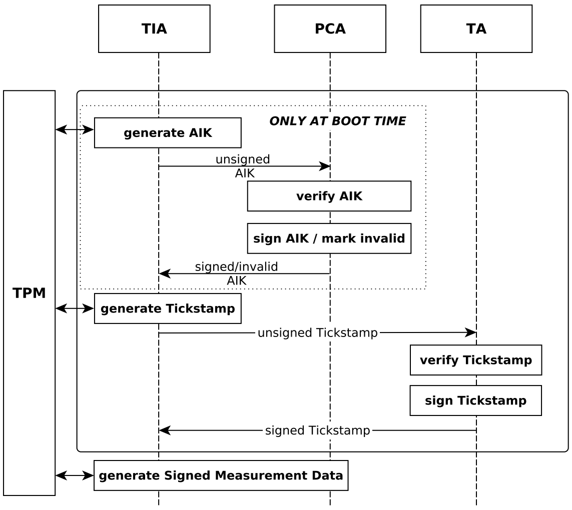


Fig. 5: Process model

Figure 5 shows the interactions between TIA and the trusted third party services PCA and TA, as well as the role of the TPM within the TIA. The more elaborate tasks of establishing trusted time and a trusted signature have to be accomplished only once during device initialization.

4 Scalability of Trust Establishment in Distributed SCADA Systems

The establishment of a trust concept for CPS requires the utilization of cryptographic techniques and, hence, the need to process data like hash values, time stamps, or digital signatures in addition to the sensor measurements. This may lead to a significant increase of the amount of data to be transmitted over the network and processed by the SCADA control station. Care must be taken that the security-related data overhead is kept within reasonable limits in order to guarantee uncompromised processing of the sensor data.

In this section, the essential scalability aspects of our trust concept are analyzed. While the sensors used in our dam scenario are fairly simple devices, there is a growing use of highly complex sensoring devices, e.g., in automotive assistance systems [41]. Such systems are based on embedded versions of standard operating systems [15], e.g., linux, or even on smartphone platforms, e.g., Android. Since the essence of our trust concept is the revelation of software manipulation, such complex sensors are in the focus of the scalability analysis. Whenever complex sensors are involved in a system, the existence of software flaws has to be taken into account. Reliable operation of such sensors typically requires occasional software updates, e.g., security patches. As a consequence, the sensor systems cannot be assumed to be static and a trust concept has to provide an adequate re-verification mechanism for the case of updates.

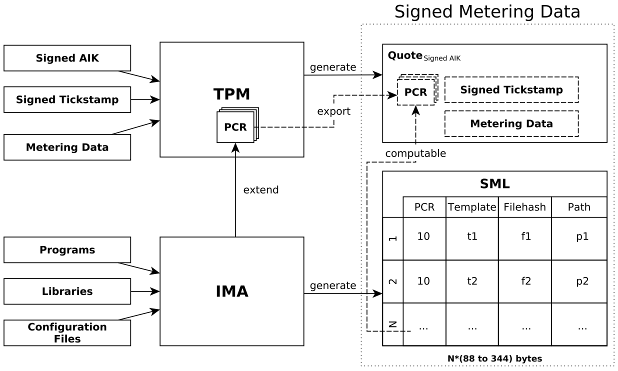
Based upon a more detailed description of the software attestation process the security-related data structures are investigated and quantified in 4.1. The computational costs of the proposed trust scheme have been evaluated using a prototypical implementation relying on the *Integrity Measurement Architecture (IMA)* [34] for system integrity measurement. The evaluation results are discussed in 4.2. We then propose a scalable trust establishment concept and present corresponding algorithms for the generation and verification of trusted sensor data in 4.3.

4.1 Quantitative Analysis of Security-related Data

According to [25] and [29], two principal data structures are needed for trusted data acquisition:

TPM Quote. A Quote is the result of a special TPM "quote" operation generating an approved sensor value. It contains (1) a time stamp approved by the trusted Time Authority, (2) hash values for the verification of the system integrity measurement results, and (3) the sensor data. The Quote is signed with the TPM's PCA-approved AIK. The hash values (aka *PCR values*) for checking the system integrity measurement results are stored in the TPM's manipulation-protected *Platform Configuration Registers (PCRs).*

*Stored Measurement Log (*SML*).* The SML is a log file including all values necessary to verify the current system state. It is generated by the Integrity Measurement Architecture. The SML contains all values necessary to reconstruct the PCRs included in the generated Quote and can be obtained directly from the system through a system kernel interface.



	PCR	Template	Filehash	Path
1	10	t1	f1	p1
2	10	t2	f2	p2
N	...	...	...	...

Fig. 6: Quote and SML Generation Process

Figure 6 shows the generation of signed sensor data as introduced in Figure 4 based on Quotes, SML and PCR values. Within the scope of system integrity measurement, the IMA measures each software component by computing a hash value, recording the result as a new SML entry, and performing a TPM "extend" operation extending a hash chain

Table 2: SML Measurements

SML Entries	100	500	1000	5000	10000
File Size	12 KB	60 KB	127 KB	676 KB	1.4 MB
(1) PCR Verification	0.31 ms	1.60 ms	3.42 ms	16.07 ms	33.17 ms
(2) Template Verification	6.42 ms	35.43 ms	70.8 ms	342.99 ms	680.63 ms
(3) Hash Verification	0.262 s	1.356 s	2.741 s	13.308 s	26.778 s
Complete Verification	0.296 s	1.671 s	3.402 s	15.229 s	30.717 s

with a hash of the new SML entry. The last hash value of this chain is always stored in a manipulation-protected PCR.

The size of a Quote is the size of the sensor data plus some fixed overhead for the other Quote components. The SML is a rather large list growing continuously during system runtime. Each intermediate system state creates a new SML entry containing hash values and the file system path of the hashed software component. Depending on the length of the path, the size of an SML entry varies from 88 to 344 Bytes. In practice, the SML size varies from a couple of KB, right after system start-up, up to certain MB depending on (i) runtime, (ii) type, and (iii) measured intermediate states of the system. On our evaluation system the size for 10.000 SML entries was approximately 1.4 MB. However, for sensors, running a limited amount of software with infrequent updates, but rather long system runtime, we expect the SML to contain 300-1000 entries.

In order to verify sensor data, the verification system needs the Quotes and the SML from the TIA. Considering the size of the SML and the large amount of sensor values processed in a SCADA system, it is quite obvious that efficiency with respect to communication bandwidth and computational effort are crucial for a practicable solution.

4.2 Computational Costs

To determine the trustworthiness of the data acquisition system, the SML must always be verified comprehensively. The hash chain approach described above uses one hash value – the last one in the chain - as a checksum for the integrity of the whole TIA system. A drawback of this approach is that the necessary verification steps cannot be parallelized, as each element of the hash chain c_{i+1} depends on the predecessor value c_i. The length of the chain is the number of entries of the SML.

Specifically, this means that even if a preceding verified trusted state was ascertained, the entire attestation process must be repeated entirely before a new sensor measurement can be accepted. To get a better understanding for the attestation process and the computational costs the process induces, we examined a common attestation scheme shown in Figure 7, which illustrates the verification of each intermediate system state. Furthermore, we provide time-based measurement results for SMLs of different dimensions in Table 2. In particular, we analyzed the verification time for SMLs with 100, 500, 1000, 5000 and 10000 entries. The attestation process was executed on a 64-Bit Intel Core I5 760 CPU@ 2.800 GHz. The measurements of (1), (2), and (3) were obtained using a python script.

As shown in Table 2, file size and verification time grow linearly with the number of SML entries. Analysis of the time-based measurement results shows that hash verification

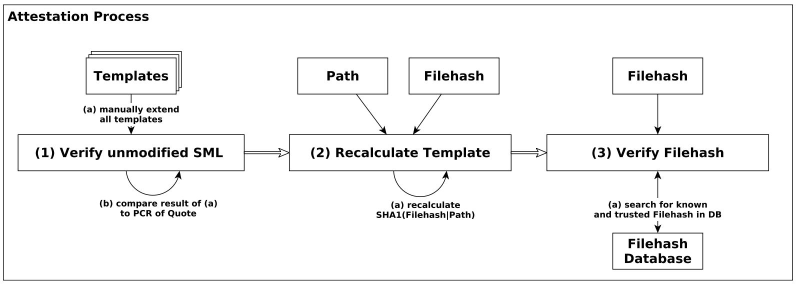

Attestation Process
Templates
(a) manually extend all templates
(1) Verify unmodified SML
(b) compare result of (a) to PCR of Quote
Path
Filehash
(2) Recalculate Template
(a) recalculate SHA1(Filehash|Path)
Filehash
(3) Verify Filehash
(a) search for known and trusted Filehash in DB
Filehash Database

Fig. 7: Attestation Process

(3) is the critical step with respect to computational effort. Whereas (1) PCR verification steps must be performed strictly sequential, (2) template verification, and (3) hash verification can be parallelized. While we expect a parallelized computation of (2) and (3) to be notably faster than our sequential approach, it would not reduce the amount of data exchanged between TIA and verifier.

4.3 Scalable Data Generation and Verification

In the following, we propose a scalable attestation algorithm composed of the TIA part in Algorithm 1 and the verifier part in Algorithm 2.

Algorithm 1 TIA: Signed Measurement Data Generation Scheme

```
Require: $i = 0, c_i = 0$
  function $generate\_sensor\_measurement(\,)$
    $q_i = get\_quote()$
    $sml_i = get\_sml()$
    $store\_sml\_count(c_i)$
    if $i == 0$ then
      $send\_sensor\_measurement(q_i, sml_i)$
    else
      $\delta_{sml_{i-1}:sml_i} = truncate\_sml\_until(c_{i-1})$
      $send\_sensor\_measurement(q_i, \delta_{sml_{i-1}:sml_i})$
    end if
    $increment(i)$
  end function
```

The central idea is that the TIA transmits the entire SML only with the first Quote. On any subsequent execution, the SML sml_i is truncated until the last known line c_i. This generates our subsequent SML-delta $\delta_{sml_{i-1}:sml_i} = truncate\_sml\_until(c_{i-1})$, which replaces the complete SML that is transmitted to the verifier, reducing the amount of transferred data to a minimum.

Consequently, the verifier only needs to recalculate the templates of the changed SML entries $\delta_{sml_{i-1}:sml_i}$, which significantly reduces computational effort. However, we

Algorithm 2 Verifier: Signed Measurement Data Verification Scheme

```
Require: $h_{aik}, quote_i, sml_i, AIK_{pub}$
  function $verify\_sensor\_measurement(quote_i, sml_i)$
      if $verify\_quote(quote, AIK_{pub})$ then
          if $verify\_sml(sml_i, h_{aik})$ then
              $h_{aik} = extract\_hash(quote_i)$
              return "$TRUSTED$"
          else
              $h_{aik} =$ ""                                          ▷ Reset $h_{aik}$
              return "$UNTRUSTED$"
          end if
      end if
      return "$UNTRUSTED$"
  end function
```

expect additional SML entries to appear on very rare occasions, basically only after designated software updates or in case an attack happened. Hence, in most subsequent attestation processes, $\delta_{sml_{i-1}:sml_i}$ can be omitted entirely, or will only comprise a couple of new entries, which renders the computational effort negligible.

In order to make this scheme work, the verifier stores the last known trusted hash value in a tuple $\{AIK \rightarrow h_{aik}\}$ for the least known state of the TIA. Then, $\delta(sml_{i-1} : sml_i)$ is sufficient to synchronize the verifier's SML with the changed TIA's SML and to verify the current system state without recalculation of the entire SML sml_i, necessary without the modifications made.

5 Background and Related Work

Dam monitoring applications with Automated Data Acquisition System (ADAS) are discussed in [26, 22]. Usually, an ADAS is organized as a SCADA system with a hierarchical organisation (cf. Figure 2). Details on SCADA systems organisation can be found in [6, 5]. In the majority of cases, SCADA systems have very little protection against the escalating cyber threats. Compared to traditional IT systems, securing CPS poses unique challenges. In order to understand those challenges and the potential danger, [42] provides a taxonomy of possible cyber attacks including cyber-induced cyber-physical attacks with respect to SCADA systems. Specific SCADA related security problems are discussed in [8]. An overview of the challenges and the current state-of-the-art in modeling CPS in general is given in [9].

Besides identification of security requirements, the further security engineering process has to address issues such as how to mitigate risks resulting from connectivity and how to integrate security into a target architecture [2]. In [16], some of the open issues in future energy networks are discussed and a vision of a security infrastructure for such networks built on hardware security anchors is described. In [1], a framework for the protection of energy control systems is introduced that integrates different state-of-the-art technologies in order to improve status management, anomaly prevention, and security. In [13], security, trust and quality of service requirements in next-generation control and communication for large power systems are examined and the GridStat middleware framework addressing these requirements is introduced. In [38], vulnerabilities of current SCADA systems are described and a suite of security protocols to provide authenticated channels optimized for SCADA systems is proposed.

Specific mechanisms for enforcement of authenticity requirements that have been derived by the method proposed in this article are based on integration of TC concepts into CPS systems. The key concept of TC [21] is the extension of trust from a root of trust (such as the TPM) to further system components [36]. This concept ensures that a system is and remains in a predictable and trustworthy state and thus produces authentic results. An approach for the generation of secure evidence records was presented in [29]. This approach, which was the basis for our proof-of-concept implementation in [7], makes use of established hardware-based security mechanisms for special data recording devices. Our work presented here, additionally analysed scalability properties of the approach by measurements of overhead for trust establishment and suggest efficient schemes for evidence generation and evidence verification.

For secure evidence generation, those parts of the TPM that identify the device, bind data to the identity of the device, and provide authentic reports on the current state of the device are essential [29]. Evidence collectors can add semantic information to the evidence record and make it available for distribution and storage [28, 27]. The cumulative attestation proposed by LeMay and Gunter [19] provides additional records and attests to the history of the boot process. In the context of digital cameras, the feasibility of the use of TPMs for the protection of digital images has already been proposed [29] and demonstrated [39]. In [35], advanced schemes allowing for scalable attestation have been proposed. In CPS it can also be necessary to establish a peer-to-peer structure without any central node. In order to ensure that all events can be ordered by time, the synchronisation of time ticks can be combined with other existing security mechanisms [20]. General properties of time synchronisation protocols and algorithms have been analysed in [12].

Security information and event management (SIEM) systems [24] are generic consumers of sensor events. From the architectural perspective of a SIEM system, the TIA implements a specific software appliance residing in edge payload nodes. Based on the requirements of CPS for novel SIEM architectures [30], in the European project MASSIF [31] we developed the TIA that implements a MASSIF compliant remote smart sensor, which provides authenticated component event reporting [23]. The trustworthiness of the information from the TIA is indispensable, when process control in critical infrastructures is dependent on this information. We have shown this in applications reported in [32] on misuse case scenarios from the hydroelectric power plant introduced in Section 2. In addition to integrity and authenticity provided by the TIA, it is important to enforce a resilient communication among the edge devices and core nodes of a SIEM infrastructure. In the MASSIF architecture, a resilient event bus [23] provides several mechanisms and routing strategies to deliver messages in a secure and timely way. We assume that in addition to the use in generic SIEM systems, the TIA scalability concept proposed in this work can also be applied in specific agent-based architectures, such as the autonomic agent trust model proposed in [40].

6 Conclusion and Future Work

With the emerging CPS demanding new security challenges arise at the interface between the cyber and physical world. In particular, the geographically dispersed placement of sensors and actuators in non-protected environments makes them vulnerable for various attacks with possibly disastrous impact on critical infrastructures and their human users.

Protection of CPS against those attacks is a multifaceted complex task. In this paper, we addressed three important aspects related to this task based on a model of a typical cyber-physical application scenario, a hydro-electric powerplant.

Firstly, the elicitation of critical security requirements has been investigated. We used a model-based approach to systematically identify security requirements in CPS. The action-oriented approach considers control flow and information flow between interdependent actions, in particular, the boundary actions, which represent the interaction of the physical with the cyber world. Secondly, we developed the TIA, a holistic protection concept for critical event sources, particularly addressing the problem of unrevealed software manipulation. Finally, we analysed scalability properties of the TIA approach and presented scalable trust establishment algorithms.

We envision to extend the TIA approach to other types of devices, which are known to be critical for trusted monitoring within CPS. Particularly, we think of network devices, which often also operate in unprotected environments. The software complexity of such devices is comparable to the smart sensors and Trusted Computing concepts should be applicable for their protection.

Acknowledgement

Roland Rieke, Nicolai Kuntze, and Luigi Coppolino developed the work presented here in the context of the project MASSIF (ID 257475) being co-funded by the European Commission within FP7.

References

1. Alcaraz, C., Lopez, J., Zhou, J., Roman, R.: Secure SCADA framework for the protection of energy control systems. Concurrency and Computation: Practice and Experience 23(12), 1431–1442 (2011)
2. Bodeau, D.J.: System-of-Systems Security Engineering. In: In Proc. of the 10th Annual Computer Security Applications Conference, Orlando, Florida. pp. 228–235. IEEE Computer Society (1994)
3. Bohli, J.M., Langendörfer, P., Skarmeta, A.F.: Security and privacy challenge in data aggregation for the iot in smart cities. In: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, pp. 225–244. River Publishers (2013)
4. Choi, J., Shin, I., Seo, J., Lee, C.: An Efficient Message Authentication for Non-repudiation of the Smart Metering Service. Computers, Networks, Systems and Industrial Engineering, ACIS/JNU International Conference on 0, 331–333 (2011)
5. Coppolino, L., D'Antonio, S., Romano, L., Spagnuolo, G.: An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies. In: Critical Infrastructure (CRIS), 2010 5th International Conference on. pp. 1–8 (sept 2010)

6. Coppolino, L., D'Antonio, S., Romano, L.: Dependability and resilience of computer networks (SCADA cybersecurity). In: CRITICAL INFRASTRUCTURE SECURITY: Assessment, Prevention, Detection, Response. WIT press (in press)
7. Coppolino, L., Jäger, M., Kuntze, N., Rieke, R.: A Trusted Information Agent for Security Information and Event Management. In: ICONS 2012, The Seventh International Conference on Systems, February 29 - March 5, 2012, Reunion Island, pp. 6–12. IARIA (2012)
8. Dan, G., Sandberg, H., Ekstedt, M., Björkman, G.: Challenges in power system information security. IEEE Security & Privacy 10(4), 62–70 (2012)
9. Derler, P., Lee, E.A., Sangiovanni-Vincentelli, A.: Modeling cyber-physical systems. Proceedings of the IEEE (special issue on CPS) 100(1), 13 – 28 (January 2012)
10. Gao, J., Xiao, Y., Liu, J., Liang, W., Chen, C.L.P.: A survey of communication/networking in smart grids. Future Generation Comp. Syst. 28(2), 391–404 (2012)
11. Gerlach, M.: Trusted Network on Wheels . ERCIM News (63), 32–33 (10 2005)
12. Gladyshev, P., Patel, A.: Formalising Event Time Bounding in Digital Investigations. International Journal of Digital Evidence (2005)
13. Hauser, C.H., Bakken, D.E., Dionysiou, I., Gjermundrød, K.H., Irava, V.S., Helkey, J., Bose, A.: Security, trust, and qos in next-generation control and communication for large power systems. IJCIS 4(1/2), 3–16 (2008)
14. Hawley, M., Howard, P., Koelle, R., Saxton, P.: Collaborative security management: Developing ideas in security management for air traffic control. In: Proceedings of 2013 International Conference on Availability, Reliability and Security, ARES 2013, pp. 808–806. IEEE Computer Society (2013)
15. IBM: A strategic approach to protecting scada and process control systems. Tech. rep., IBM Corporation (2007), `http://www.iss.net/documents/whitepapers/SCADA.pdf`, [Online; accessed 13-May-2015]
16. Kuntze, N., Rudolph, C., Cupelli, M., Liu, J., Monti, A.: Trust infrastructures for future energy networks. In: Power and Energy Society General Meeting - Power Systems Engineering in Challenging Times (2010)
17. Kuntze, N., Mähler, D., Schmidt, A.U.: Employing Trusted Computing for the forward pricing of pseudonyms in reputation systems. In: Axmedis 2006, Proceedings of the 2nd International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution, Volume for Workshops, Industrial, and Application Sessions (2006)
18. Kuntze, N., Rudolph, C.: Secure digital chains of evidence. In: Sixth International Workshop on Systematic Approaches to Digital Forensic Engeneering (2011)
19. LeMay, M., Gunter, C.: Cumulative attestation kernels for embedded systems. Computer Security–ESORICS 2009 pp. 655–670 (2009)
20. Liu, J., Yu, F., C.-H., L., Tang, H.: Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks. IEEE Transactions on Wireless Communications 8(2) (2009)
21. Mitchell, C.: Trusted Computing. Institution of Electrical Engineers (2005)
22. Myers, B.K., Dutson, G.C., Sherman, T.: Utilizing Automated Monitoring for the Franzen Reservoir Dam Safety Program. In: 25th USSD Annual Meeting and Conference Proceedings (2005) (2005)
23. Neves, N., Kuntze, N., Sarno, C.D., Vianello, V., et al.: Resilient SIEM framework architecture, services and protocols. Deliverable D5.1.4, FP7-257475 MASSIF European project (September 2013)
24. Nicolett, M., Kavanagh, K.M.: Magic Quadrant for Security Information and Event Management. Gartner Reasearch (May 2010)
25. Oberle, A., Rein, A., Kuntze, N., Rudolph, C., Paatero, J., Lunn, A., Racz, P.: Integrating trust establishment into routing protocols of today's MANETs. In: Wireless Communications and Networking Conference (WCNC), 2013 IEEE. pp. 2369–2374. IEEE (2013)

26. Parekh, M., Stone, K., Delborne, J.: Coordinating Intelligent and Continuous Performance Monitoring with Dam and Levee Safety Management Policy. In: Association of State Dam Safety Officials,Proceedings of Dam Safety Conference 2010 (2010)
27. Pollitt, M.: Report on digital evidence. In: 13th INTERPOL Forensic Science Symposium. Citeseer (2001)
28. Reith, M., Carr, C., Gunsch, G.: An examination of digital forensic models. International Journal of Digital Evidence 1(3), 1–12 (2002)
29. Richter, J., Kuntze, N., Rudolph, C.: Security Digital Evidence. In: 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering. pp. 119–130. IEEE (2010)
30. Rieke, R., Coppolino, L., Hutchison, A., Prieto, E., Gaber, C.: Security and reliability requirements for advanced security event management. In: Proc. of the 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS'12), St. Petersburg, Russia. LNCS, vol. 7531, pp. 171–180. Springer (October 2012)
31. Rieke, R., Prieto, E., Diaz, R., Debar, H., Hutchison, A.: Challenges for advanced security monitoring – the MASSIF project. In: Fischer-Hübner, S., Katsikas, S., Quirchmayr, G. (eds.) Trust, Privacy and Security in Digital Business, Lecture Notes in Computer Science, vol. 7449, pp. 222–223. Springer Berlin / Heidelberg (2012)
32. Rieke, R., Repp, J., Zhdanova, M., Eichler, J.: Monitoring security compliance of critical processes. In: Parallel, Distributed and Network-Based Processing (PDP), 2014 22th Euromicro International Conference on. pp. 525–560. IEEE Computer Society (Feb 2014)
33. Russell, S.J., Norvig, P.: Artificial Intelligence: A Modern Approach. Pearson Education, 2 edn. (2003)
34. Sailer, R., Zhang, X., Jaeger, T., Van Doorn, L.: Design and implementation of a tcg-based integrity measurement architecture. In: USENIX Security Symposium. vol. 13, pp. 223–238 (2004)
35. Stumpf, F., Fuchs, A., Katzenbeisser, S., Eckert, C.: Improving the Scalability of Platform Attestation. In: Proceedings of the Third ACM Workshop on Scalable Trusted Computing (ACM STC'8). pp. 1–10. ACM Press, Fairfax, USA (October 31 2008)
36. Trusted Computing Group TPM Working Group: TCG Specification Architecture Overview. http://www.trustedcomputinggroup.org/resources/ (2007)
37. Wang, W., Xu, Y., Khanna, M.: A survey on the communication architectures in smart grid. Computer Networks 55(15), 3604–3629 (2011)
38. Wang, Y.: sscada: Securing SCADA infrastructure communications. CoRR abs/1207.5434 (2012), `http://arxiv.org/abs/1207.5434`
39. Winkler, T., Rinner, B.: TrustCAM: Security and Privacy-Protection for an Embedded Smart Camera based on Trusted Computing. In: Proceedings of the Conference on Advanced Video and Signal-Based Surveillance (2010)
40. Xu, X., Bessis, N., Cao, J.: An autonomic agent trust model for iot systems. Procedia Computer Science 21, 107 – 113 (2013), the 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013) and the 3rd International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH)
41. Zaldivar, J., Calafate, C.T., Cano, J.C., Manzoni, P.: Providing accident detection in vehicular networks through obd-ii devices and android-based smartphones. In: Local Computer Networks (LCN), 2011 IEEE 36th Conference on. pp. 813–819. IEEE (2011)
42. Zhu, B., Joseph, A., Sastry, S.: A taxonomy of cyber attacks on scada systems. In: Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. pp. 380–388. ITHINGSCPSCOM '11, IEEE Computer Society, Washington, DC, USA (2011)